III. REMARKS

Claims 1-16 are not unpatentable under 35 U.S.C. §103 over Jones in view of Arazi.

Independent claims 1 and 13 have been amended to more clearly recite that the headset and the mobile station are separate from each other and communicate wirelessly.

First and mainly, neither Jones, nor Arazi teach the presence of such a media player in the headset which would **decode** stored files as recited in claims 1 and 13. The micro control mp3 block 68 (shown in Fig. 4 in Jones) does not reside in the heasdset 12 but in the control unit 18.

Secondly, the skilled person would not have replaced the cable between parts 12 and 18 in Jones with the Bluetooth connection disclosed by Arazi. Nowhere in Jones is there a teaching that parts 12 and 18 should wirelessly communicate as recited in claims 1 and 13.

In fact, there are at least two facts that actually discourage the replacement of the cable between parts 12 and 18 of Jones with a wireless connection:

1) Bluetooth was first introduced already in 1994 (see the other enclosure from Wikipedia network encyclopedia). Jones' priority date is many years after it and the inventor was surely aware of Bluetooth when inventing his invention. If it was so obvious to replace the wired connection between parts 12 and 18 with a wireless one, why does Jones not say that?
2) Jones already mentions a wireless connection, but this is between the watch 72 and part 18. Again, if it was so obvious to replace the connection between parts 12 and 18 with a wireless one, why does Jones not say that, although in other places in the document he mentions wireless connections?

Thirdly, even if the wired connections between parts 12 and 18 had been replaced by a wireless connection, one would not have arrived at the invention as recited in claims 1 and 13. Namely, the decoding of files in Jones occurs in part 18. However, the present claims require the decoding to occur on the headset. But, as described earlier, no decoding occurs in the headset part 12 in Jones.

Furthermore, it is respectfully submitted that the Examiner's comments in the continuation sheet of the Advisory Action are erroneous.

First of all speakers and amplifiers have nothing to do with decoding. The decoding in Jones does not occur in the headset but in the control unit 18 (as previously argued).

Secondly, "audio related functions" are not the same as "decoding". A volume control, for example, is an audio related function, which does not contain decoding.

Thirdly, the place where a digital music source is placed does not determine where the music content is decoded. Although the headset in Jones has a slot for a 32-Megabyte module that has encoded mp3 music, this does not mean that the music files are decoded in the headset. To the contrary, it is certain that since the mp3 decoder block 68 resides in the control unit 18, this is where the decoding occurs, not in the headset 12.

In summary, it is not obvious to combine the references since Bluetooth and other wireless connections were known to Jones, which even discloses one. Further, even if the references are somehow combined, the result is not the claimed invention since the claimed decoding in the headset feature would still be missing.

Thus the rejection of claims 1-16 should be withdrawn.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for the RCE and extension of time fee ($910.00) as well as any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Joseph W. Gamberdell
Reg. No. 44,695

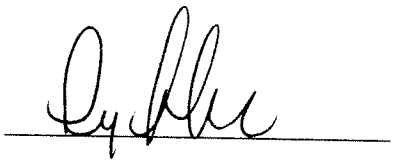
20 Agosto 2006
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being transmitted electronically, on the date indicated below, addressed to the Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 20 October 2006

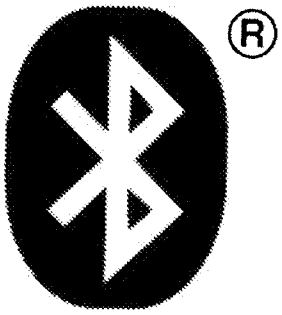
Signature: 

Lisa Shimizu
Person Making Deposit

Bluetooth

From Wikipedia, the free encyclopedia

Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency.



Bluetooth logo

Contents

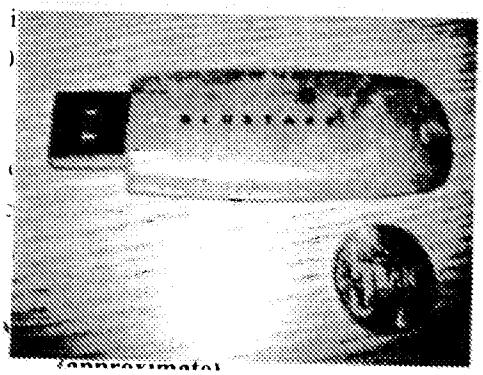
Etymology

The name Bluetooth is derived from the cognomen of a 10th century king of Denmark, Harald Bluetooth. According to the inventors of the Bluetooth technology, Harald engaged in diplomacy which led warring parties to negotiate with each other, making *Bluetooth* a fitting name for their technology, which allows different devices to talk to each other.

Introduction

Bluetooth is a radio standard and communications protocol pri
with a short range (power class dependent: 1 metre, 10 metres,
microchips in each device.

Bluetooth lets these devices communicate with each other whe
communications system, so they do not have to be in line of si
rooms, so long as the received transmission is powerful enougl



A typical Bluetooth USB adapter

Class	Maximum Permitted Power (mW)	Maximum Permitted (dBm)	
Class 1	100 mW	20 dBm	
Class 2	2.5 mW	4 dBm	~10 metres
Class 3	1 mW	0 dBm	~1 metre

Bluetooth applications

- Wireless control of and communication between a cell phone and a hands free headset or car kit. This is the most popular use.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communications with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files between devices via OBEX.
- Transfer of contact details, calendar appointments, and reminders between devices via OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers and medical equipment.
- For remote controls where infrared was traditionally used.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless control of a games console, Nintendo's Wii and Sony's PlayStation 3 will both use Bluetooth technology for their wireless controllers.
- Sending commands and software to the LEGO Mindstorms NXT instead of infrared.

Bluetooth vs. Wi-Fi in today's networked world

Bluetooth and Wi-Fi both have their places in today's offices, homes and on the move: setting up networks, printing, or transferring presentations and files from PDAs to computers.

Bluetooth

Bluetooth is in a variety of new products such as phones, printers, modems, and headsets, to name a few. Bluetooth is acceptable for situations when two or more devices are in close proximity with each other and don't require high bandwidth. Bluetooth is most commonly used with cell phones and handheld computing devices, either using a Bluetooth headset or transferring files from phones/PDAs to computers. Since Bluetooth uses short-range radio frequencies, it is not as effective for setting up networks that can be accessed

from remote locations as with Wi-Fi.

Bluetooth also simplified the discovery and setup of services. Wi-Fi is more analogous to the traditional Ethernet network, and requires configuration to set up shared resources, transmit files, set up audio links (e.g. headsets and hands-free devices), whereas Bluetooth devices advertise all services they actually provide; this makes the utility of the service that much more accessible, without the need to worry about network addresses, permissions and all the other considerations that go with typical networks.

Wi-Fi

Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power consumption resulting in a stronger connection. As mentioned earlier, Wi-Fi is sometimes called "wireless ethernet". Although this description is inaccurate, it provides an indication of Wi-Fi's capabilities. Wi-Fi is better suited for setting up networks as it enables a faster connection and has better security than Bluetooth. Wi-Fi is also becoming increasingly popular and widespread; it is a standard feature of most new laptop computers, and is a straightforward expansion to desktop computers not already Wi-Fi enabled (eg. through the use of a USB dongle).

As a traditional networking medium, Wi-Fi is more versatile, but harder to configure. Most users need good know-how (or an IT department) to get things set up, especially when using more obscure services such as audio and HID. For this reason, Wi-Fi falls well short of the standard for ad-hoc networking, one of the basic tenets of the Bluetooth framework. [1] (http://www.bluetooth.com/Bluetooth/Learn/Benefits/)

One method for comparing the efficiency of wireless transmission protocols such as Bluetooth and Wi-Fi is called spatial capacity.

Specifications and Features

The Bluetooth specification was first developed in 1994 by Jaap Haartsen, who was working for Ericsson Radio Systems located in Emmen in The Netherlands. The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has over 6000 companies worldwide. It was established by Ericsson, Sony Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies as Associate or Adopter members. Bluetooth is also known as IEEE 802.15.1.

Bluetooth 1.0 and 1.0B

Versions 1.0 and 1.0 B had many problems and the various manufacturers had great difficulties in making their products interoperable. 1.0 and 1.0B also had mandatory Bluetooth Hardware Device Address (BD_ADDR) transmission in the handshaking process, rendering anonymity impossible at a protocol level, which was a major setback for services planned to be used in Bluetooth environments, such as Consumerium.

Bluetooth 1.1

- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.

- *Received Signal Strength Indicator (RSSI)*

Bluetooth 1.2

This version is backwards compatible with 1.1 and the major enhancements include

- *Adaptive Frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence
- *Higher transmission speeds* in practice
- *extended Synchronous Connections (eSCO)*, which improves voice quality of audio links by allowing retransmissions of corrupted packets.
- *Host Controller Interface (HCI) support for 3-wire UART*
- *HCI access to timing information* for Bluetooth applications:

Bluetooth 2.0

This version is backwards compatible with 1.x. The main enhancement is the introduction of *Enhanced Data Rate (EDR)* of 3.0 Mbps. This has the following effects (Bluetooth SIG, 2004):

- 3 times faster transmission speed (up to 10 times in certain cases).
- Lower power consumption through a reduced duty cycle.
- Simplification of multi-link scenarios due to more available bandwidth.
- Further improved BER (bit error rate) performance.

Future of Bluetooth

The next version of Bluetooth technology, currently code-named Lisbon, includes a number of features to increase security, usability and value of Bluetooth. The following features are defined:

- Atomic Encryption Change - allows encrypted links to change their encryption keys periodically, increasing security, and also allowing role switches on an encrypted link.

- Extended Inquiry Response - provides more information during the inquiry procedure to allow better filtering of devices before connection. This information includes the name of the device, and a list of services, with other information.

- Sniff Subrating - reducing the power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most, with mice and keyboards increasing the battery life from 3 to 10 times those currently used.

- QoS Improvements - these will enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.

- Simple Pairing (http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf) - this improvement will radically improve the pairing experience for Bluetooth devices, while at the same time increasing the use and strength of

security. It is expected that this feature will significantly increase the use of Bluetooth.

Bluetooth technology already plays a part in the rising Voice over IP (VOIP) scene, with Bluetooth headsets being used as wireless extensions to the PC audio system. As VOIP becomes more popular, and more suitable for general home or office users than wired phone lines, Bluetooth may be used in Cordless handsets, with a base station connected to the Internet link.

The version of Bluetooth after Lisbon, code-named Seattle, has many of the same features, but is most notable for plans to adopt Ultra-wideband radio technology. This will allow Bluetooth use over UWB radio, enabling very fast data transfers, synchronizations and file pushes, while building on the very low power idle modes of Bluetooth. The combination of a radio using little power when no data is transmitted, and a high data rate radio used to transmit bulk data, could be the start of software radios. Bluetooth, given its worldwide regulatory approval, low power operation, and robust data transmission capabilities, provides an excellent signalling channel to enable the soft radio concept.

On 28 March 2006, the Bluetooth Special Interest Group (SIG) announced its selection of the WiMedia Alliance Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) version of Ultra-wideband (UWB) for integration with current Bluetooth wireless technology. UWB integration will create a version of the globally popular Bluetooth wireless technology with a high speed/high data rate option. This new version of Bluetooth technology will meet the high-speed demands of synchronizing and transferring large amounts of data as well as enabling high quality video and audio applications for portable devices, multi-media projectors and television sets, wireless VOIP. At the same time, Bluetooth technology will continue catering to the needs of very low power applications such as mice, keyboards and mono headsets, enabling devices to select the most appropriate physical radio for the application requirements, thereby offering the best of both worlds.

Technical information

Communication & connection

A Bluetooth device playing the role of the "master" can communicate with up to 7 devices playing the role of the "slave". This network of "group of up to 8 devices" (1 master + 7 slaves) is called a piconet. A piconet is an ad-hoc computer network of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices (because a three-bit MAC address is used). Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time.

At any given time, data can be transferred between the master and 1 slave; but the master switches rapidly from slave to slave in a round-robin fashion. (Simultaneous transmission from the master to multiple slaves is possible, but not used much in practice). Either device may switch the master/slave role at any time.

Bluetooth specification allows connecting 2 or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another piconet. These devices have yet to come, though are supposed to appear in 2007.

Setting up connections

Any Bluetooth device will transmit the following sets of information on demand:

- Device Name
- Device Class
- List of services
- Technical information eg: device features, manufacturer, Bluetooth specification, clock offset

Anything may perform an "inquiry" to find other devices to which to connect, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device it will always respond to direct connection requests and will transmit the information shown in the list above if requested for it. Use of the device's services however may require pairing or its owner to accept but the connection itself can be started by any device and be held until it goes out of range. Some devices can only be connected to one device at a time and connecting to them will prevent them from connecting to other devices and showing up in inquiries until they disconnect the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries and instead friendly "Bluetooth names" are used which can be set by the user, and will appear when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops will only show the Bluetooth names and special programs are required to get additional information about remote devices. This can get confusing as, for example, there could be several phones in range named "T610" (see "Bluejacking").

Pairing

Pairs of devices may establish a trusted relationship by learning (by user input) a shared secret known as a "passkey". A device that wants to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt the data that they exchange over the air so that no one can listen in. The encryption can however be turned off and passkeys are stored on the device's file system and not the Bluetooth chip itself. Since the Bluetooth address is permanent a pairing will be preserved even if the Bluetooth name is changed. Pairs can be deleted at any time by either device. Devices will generally require pairing or will prompt the owner before it allows a remote device to use any or most of its services. Some devices such as Sony Ericsson phones will usually accept OBEX business cards and notes without any pairing or prompts. Certain printers and access points will allow any device to use its services by default much like unsecured Wi-Fi networks.

Air interface

The protocol operates in the license-free ISM band at 2.45 GHz. In order to avoid interfering with other protocols which use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels up to 1600 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature *Bluetooth Enhanced Data Rate (EDR)*, and thus reach 2.1 Mbit/s. Technically version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing consumption to half that of 1.x devices

(assuming equal traffic load).

Bluetooth differs from Wi-Fi in that the latter provides higher throughput and covers greater distances but requires more expensive hardware and higher power consumption. They use the same frequency range, but employ different multiplexing schemes. While Bluetooth is a cable replacement for a variety of applications, Wi-Fi is a cable replacement only for local area network access. Bluetooth is often thought of as wireless USB whereas Wi-Fi is wireless Ethernet, both operating at much lower bandwidth than the cable systems they are trying to replace. However, this analogy is not accurate since unlike USB, Bluetooth does not require the presence of a host PC.

Many USB Bluetooth adapters are available, some of which also include an IrDA adapter.

Older (pre-2003) Bluetooth adapters, however, limit the amount of services by offering only the Bluetooth Enumerator and a less-powerful incarnation of Bluetooth Radio. Such devices are able to link computers via Bluetooth, but they unfortunately don't offer much in the way of the twelve or more services that modern adapters are able to utilize.

Security

Security measures

Bluetooth uses the SAFER+ algorithm for authentication and key generation. The E0 stream cipher is used for encrypting packets. This makes eavesdropping on Bluetooth-enabled devices more difficult.

Security concerns

2003:
In November 2003, Ben and Adam Laurie from A.L. Digital Ltd. (http://www.thebunker.net/index.html) discovered that serious flaws in Bluetooth security may lead to disclosure of personal data (see http://bluestumbler.org). It should be noted however that the reported security problems concerned some poor implementations of Bluetooth, rather than the protocol itself.

In a subsequent experiment, Martin Herfurt from the trifinite.group (http://trifinite.org/trifinite_group.html) was able to do a field-trial at the CeBIT fairgrounds showing the importance of the problem to the world. A new attack called BlueBug (http://trifinite.org/trifinite_stuff_bluebug.html) was used for this experiment.

2004:
In April 2004, security consultant firm @Stake (http://www.atstake.com/) (now Symantec) revealed a security flaw that makes it possible to crack into conversations on Bluetooth based wireless headsets by reverse engineering the PIN.

This is one of a number of concerns that have been raised over the security of Bluetooth communications. In 2004 the first **purported** virus using Bluetooth to spread itself among mobile phones appeared (http://www.theregister.co.uk/2004/06/15/symbian_virus/) for the Symbian OS. The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate.

Note: the virus was written as a proof-of-concept by a group of virus writers known as 29A and sent to

anti-virus groups. Thus it should be regarded as a **potential** (but NOT real) security threat of Bluetooth or Symbian OS as the virus has never spread in the wild.

In August 2004, a world-record-setting experiment (http://trifinite.org/trifinite_stuff_lds.html) (see also Bluetooth sniping) showed that the range of class 2 Bluetooth radios could be extended to 1.78 km (1.08 mile) with directional antennas. This poses a potential security threat as it enables attackers to access vulnerable Bluetooth-devices from a distance beyond expectation. However, such experiments will not work using signal amplifiers as the attacker must also be able to receive information from its victim in order to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on.

2005:
In April 2005, Cambridge University security researchers published results (http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf) of their actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, confirming the attacks to be practicably fast and Bluetooth's symmetric key establishment method to be vulnerable. To rectify this vulnerability, they carried out an implementation which showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as handphones.

In June 2005 Yaniv Shaked and Avishai Wool published the paper "Cracking the Bluetooth PIN1" (http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html), which shows both passive and active methods for obtaining the PIN for a Bluetooth Link. The passive attack would allow a suitably equipped attacker to eavesdrop on communications and spoof if they were present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that the first method may be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter their PIN during the attack when their device prompts them to. Also, this active attack will most likely require custom hardware, as most commercially available Bluetooth Devices are not capable of the timing necessary.

In August 2005, police in Cambridgeshire, England, issued warnings (http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf) about thieves using Bluetooth-enabled phones to track other devices left in cars. Police are advising users to ensure any mobile networking connections are de-activated if laptops and other devices are left in this way. However, the best way is to not leave any valuable devices in cars.

2006:
In April 2006, researchers from Secure Network and F-Secure published a report (http://www.securenetwork.it/bluebag_brochure.pdf) which warns of the huge number of devices left in a visible state, and issued statistics on the spread of various bluetooth services and the ease of spread of an eventual bluetooth worm.

Bluetooth profiles

In order to use Bluetooth, a device must be compatible with certain Bluetooth profiles. These define the possible applications.

Origin of the name and the logo

The system is named after a Danish king Harald Blåtand (Harold I of Denmark in English, kong Harald Blåtann in Norwegian), King of Denmark and Norway from 935 and 936 respectively, to 940 known for his unification of previously warring tribes from Denmark (including Scania, present-day Sweden, where the Bluetooth technology was invented) and Norway. Bluetooth likewise was intended to unify different technologies like computers and mobile phones. The Bluetooth logo merges the Nordic runes analogous to the modern Latin H and B: and . The name may have been inspired less by the historical Harald than the loose interpretation of him in The Long Ships by Frans Gunnar Bengtsson, a Swedish best-selling Viking-inspired novel.

This logo is similar to an older logo for Beauknit Textiles, a division of Beauknit Corporation. That logo, using the obvious connection of a reversed K and B for Beauknit, is wider and has rounded corners, but is otherwise the same.

The name was originally only a code-name for the project, but ended up sticking.

Bluetooth Consortium

In 1998, Ericsson, IBM, Intel, Motorola, Nokia and Toshiba formed the consortium among themselves and adopted the code name Bluetooth for their proposed open specification. In December 1999, 3Com, Lucent Technologies, Microsoft and Motorola joined the initial founders as the promoter group. Since that time, Lucent Technologies transferred their membership to their spinoff Agere Systems and 3Com has left the Promoter group.

See also

- Bluesniping
- Cable spaghetti — a problem wireless technology hopes to solve
- *Origin of the word **Bluetooth***
- Salutation
- Service Location Protocol
- Ultra-wideband
- Universal Plug and Play
- Vehicular communication systems
- Wibree

References

- Bluetooth SIG (November 8, 2004). Bluetooth Special Interest Group Launches Bluetooth Core Specification Version 2.0 + Enhanced Data Rate (http://www.bluetooth.com/Bluetooth/Press/SIG/Bluetooth_Special_Interest_Group_Launches_Bluetoo Press release.

External links

- The Official Bluetooth® Wireless Info Site (http://www.bluetooth.com/) SIG public pages
- Bluetooth.org — The Official Bluetooth Membership Site (https://www.bluetooth.org/)
- How Bluetooth Works (http://www.howstuffworks.com/bluetooth.htm) at HowStuffWorks
- Official Linux Bluetooth protocol stack (http://www.bluez.org/)

Retrieved from "http://en.wikipedia.org/wiki/Bluetooth"

Categories: Wikipedia articles needing factual verification | Bluetooth | Networking standards | Mobile computer

---